

**WILLKIE FARR & GALLAGHER LLP**

BENEDICT HUR (SBN 224018)

bhur@willkie.com

SIMONA AGNOLUCCI (SBN 246943)

sagnolucci@willkie.com

EDUARDO SANTACANA (SBN 281668)

esantacana@willkie.com

DAVID D. DOAK (SBN: 301319)

ddoak@willkie.com

JOSHUA D. ANDERSON (SBN: 312836)

jpanderson@willkie.com

TIFFANY LIN (SBN 321472)

tlin@willkie.com

HARRIS MATEEN (SBN 335593)

hmateen@willkie.com

NAIARA TOKER (SBN 346145)

ntoker@willkie.com

One Front Street, 34<sup>th</sup> Floor

San Francisco, California 94111

Telephone: (415) 858-7400

Attorneys for Defendant

**GOOGLE LLC**

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

JOHN DOE I, et al., individually and on  
behalf of all others similarly situated,

Plaintiff,

vs.

GOOGLE LLC,

Defendant.

Case No. 3:23-cv-02431-VC  
(Consol. w/ 3:32-cv-02343-VC)

**DEFENDANT GOOGLE LLC'S MOTION  
TO DISMISS FIRST AMENDED  
COMPLAINT**

**Date:** February 22, 2024

**Time:** 10 a.m.

**Location:** Courtroom 4

**Judge:** Hon. Vince Chhabria

First Am. Complaint Filed: November 16, 2023

Consol. Complaint Filed: July 13, 2023

**TO PLAINTIFFS AND ALL ATTORNEYS OF RECORD:**

PLEASE TAKE NOTICE that the following Motion to Dismiss will be heard on February 22, 2024, at 10:00 a.m., or as soon thereafter as counsel may be heard, in Courtroom 4, 17<sup>th</sup> Floor, of the United States District Court for the Northern District of California, located at 450 Golden Gate Avenue, San Francisco, California 94102, with the Honorable Vince Chhabria presiding.

Defendant Google LLC (“Google”) will and hereby does move the Court pursuant to Federal Rule of Civil Procedure 12(b)(6) for an order dismissing the First Amended Consolidated Class Action Complaint (“FAC” or “Amended Complaint”) with prejudice because any amendment of the FAC would be futile. The Motion is based on this Notice of Motion and Motion, the Memorandum of Points and Authorities contained herein, Google’s concurrently filed Request for Judicial Notice in Support of the Motion (“RJN”) and exhibits attached thereto, the Declaration of Naiara Toker in Support of the RJN, the proposed order submitted with the RJN, all pleadings and other papers on file in this action, and any other evidence or argument that may be presented to the Court in connection with this Motion.

**STATEMENT OF ISSUES TO BE DECIDED**

Whether Plaintiffs’ FAC should be dismissed for failure to state a claim upon which relief can be granted under Federal Rule of Civil Procedure 12(b)(6), and whether the claims should be dismissed with prejudice where amendment would be futile.

Respectfully submitted,

Date: December 21, 2023

**WILLKIE FARR & GALLAGHER LLP**

By: /s/ Benedict Hur  
Benedict Hur

Attorneys for Defendant  
Google LLC

## **TABLE OF CONTENTS**

MEMORANDUM OF POINTS AND AUTHORITIES .....	1
I. INTRODUCTION .....	1
II. BACKGROUND .....	2
A. Plaintiffs Allege Only That Google Lawfully Provided the Websites With Analytics Services and Other Products to Help Their Companies. ....	2
B. The Contract Between Google and the Websites Forbade the Websites From Sending Google PII, Sensitive Information About a User, or Using PII or Sensitive Information to Advertise. ....	3
C. Plaintiffs’ Allegations .....	4
D. Procedural History .....	5
III. LEGAL STANDARD.....	5
IV. ARGUMENT.....	6
A. The heightened standard of Rule 9(b) applies .....	6
B. Plaintiffs Fail to State Wiretap Claim (Count 1) .....	7
1. The Websites’ Consent Defeats the Wiretap Claim .....	7
2. Google’s Lack of Intent is Fatal to the Wiretap Claim.....	8
C. Plaintiffs fail to state CIPA claims (Count 2).....	9
1. Google Is a Mere Vendor of an Analytics Tool to Record the Websites’ Own Interactions With Users.....	9
a. CIPA Section 631 .....	9
b. CIPA Section 632 .....	11
2. Google’s lack of intention is fatal to CIPA claims .....	11
D. Privacy Claims Should be Dismissed (Counts 3 and 4) .....	12
E. Plaintiffs’ UCL Claim Should be Dismissed (Count 5).....	13
F. Claims for Trespass to Chattels and Conversion Fail (Counts 6 and 12).....	15
1. Failure to Allege Intent .....	15

2.	No Interference with Plaintiffs’ Personal Property.....	15
3.	Plaintiffs Fail to Plausibly Allege Actual Loss.....	16
G.	Plaintiffs Fail to State a CDAFA Claim (Count 7).....	17
1.	Standing under CDAFA.....	17
2.	Plaintiffs Cannot Establish Google Knew Its Collection was Unauthorized.....	19
H.	No Breach of Contract (Count 8).....	21
1.	Alleged Breach One.....	21
2.	Alleged Breach Two.....	21
3.	Alleged Breach Three.....	22
4.	Alleged Breach Four.....	23
I.	No Breach of Implied Contract (Count 9).....	23
J.	No Breach of the Implied Covenant of Good Faith and Fair Dealing (Count 10).....	24
K.	Unjust Enrichment Is Not Cognizable (Count 11).....	25
V.	CONCLUSION.....	25

**TABLE OF AUTHORITIES**

	<b>Page(s)</b>
<b>Cases</b>	
<i>In re A.L.</i> , 38 Cal. App. 5th 15 (2019) .....	20
<i>Adler v. Community.com, Inc.</i> , 2021 WL 4805435 (C.D. Cal. Aug. 2, 2021).....	9
<i>Alderson v. United States</i> , 718 F. Supp. 2d 1186 (C.D. Cal. 2010) .....	16
<i>Apumac, LLC v. Flint Hills Int’l</i> , 2015 WL 13306128 (C.D. Cal. Feb. 6, 2015).....	6
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	5
<i>Bass v. Facebook, Inc.</i> , 394 F. Supp. 3d 1024 (N.D. Cal. 2019) .....	13
<i>Belluomini v. Citigroup, Inc.</i> , 2013 WL 3855589 (N.D. Cal. July 24, 2013).....	12
<i>Best Carpet Values, Inc. v. Google LLC</i> , 2021 WL 4355337 (N.D. Cal. Sept. 24, 2021) .....	15
<i>Byars v. Hot Topic, Inc.</i> , 656 F. Supp. 3d 1051 (C.D. Cal. 2023) .....	9
<i>Cahen v. Toyota Motor Corp.</i> , 717 F. App’x 720 (9th Cir. 2017) .....	23
<i>Calhoun v. Google LLC</i> , 526 F. Supp. 3d 605 (N.D. Cal. 2021) .....	1, 14
<i>Caraccioli v. Facebook, Inc.</i> , 167 F. Supp. 3d 1056 (N.D. Cal. 2016), <i>aff’d</i> , 700 F. App’x 588 (9th Cir. 2017) .....	12
<i>Careau &amp; Co. v. Sec. Pac. Bus. Credit, Inc.</i> , 222 Cal. App. 3d 1371 (1990) .....	24
<i>Casillas v. Berkshire Hathaway Homestate Ins.</i> , 79 Cal. App. 5th 755 (2022) .....	16
<i>Cottle v. Plaid Inc.</i> , 536 F. Supp. 3d 461 (N.D. Cal. 2021) .....	14, 18

<i>Doe v. Google LLC</i> , No. 23-cv-02431-VC, 2023 WL 6882766 (N.D. Cal. Oct. 18, 2023) .....	7
<i>Doe v. Roblox Corp.</i> , 602 F. Supp. 3d 1243 (N.D. Cal. 2022) .....	15
<i>People ex rel. DuFauchard v. U.S. Fin. Mgmt., Inc.</i> , 169 Cal. App. 4th 1502 (2009) .....	13
<i>In re Facebook</i> , 956 F.3d at 601 .....	12
<i>Gardiner v. Walmart, Inc.</i> , 2021 WL 2520103 (N.D. Cal. Mar. 5, 2021) .....	13
<i>Gonzalez v. Planned Parenthood of Los Angeles</i> , 759 F.3d 1112 (9th Cir. 2014) .....	5
<i>Gonzalez v. Uber Techs., Inc.</i> , 305 F. Supp. 3d 1078 (N.D. Cal. 2018) .....	13
<i>In re Google Assistant Privacy Litig.</i> , 457 F. Supp. 3d 797 (N.D. Cal. 2020) .....	13
<i>In re Google Inc. Cookie Placement Consumer Privacy Litig.</i> , 806 F.3d 125 (3d Cir. 2015) .....	18
<i>Gorlach v. Sports Club Co.</i> , 209 Cal. App. 4th 1497 (2012) .....	24
<i>Graham v. Noom</i> , 533 F. Supp. 3d 823 (N.D. Cal. 2021) .....	9, 10, 12
<i>Guz v. Bechtel Nat'l Inc.</i> , 24 Cal. 4th 317 (2000) .....	25
<i>Hernandez v. Hillsides, Inc.</i> , 47 Cal. 4th 272 (2009) .....	12
<i>Hidden Empire Holding, LLC v. Angelone</i> , 2023 WL 4208067 (C.D. Cal. May 10, 2023) .....	6
<i>Intel Corp. v. Hamidi</i> , 30 Cal. 4th 1348 (2003) .....	15, 16
<i>In re iPhone Application Litig.</i> , 6 F. Supp. 3d 1004 (N.D. Cal. 2013) .....	14
<i>In re iPhone Application Litig.</i> , 844 F. Supp. 2d 1040 (N.D. Cal. 2012) .....	15, 16

<i>In re iPhone Application Litig.</i> , 844 F. Supp. 2d at 1066–67 .....	19
<i>IV Sols., Inc. v. Empire Healthchoice Assurance, Inc.</i> , 2021 WL 5492974 (9th Cir. Nov. 23, 2021).....	7
<i>Jane Doe, et al. v. Google LLC</i> , 5:23-cv-02343 (N.D. Cal.).....	5
<i>John Doe I, et al. v. Google LLC</i> , 5:23-cv-02431 (N.D. Cal.).....	5
<i>Johnson v. Blue Nile, Inc.</i> , No. 20-cv-08183-LB, 2021 WL 1312771 (N.D. Cal. Apr. 8, 2021) .....	9
<i>Katz-Lacabe v. Oracle Am., Inc.</i> , 2023 WL 2838118 (N.D. Cal. Apr. 6, 2023) .....	8, 13
<i>Kearns v. Ford Motor Co.</i> , 567 F.3d 1120 (9th Cir. 2009) .....	6, 14
<i>Kurowski v. Rush Sys. for Health</i> , No. 22 C 5380, 2023 WL 4707184 (N.D. Ill. July 24, 2023) .....	17, 18, 19, 22
<i>LaCourt v. Specific Media, Inc.</i> , 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011) .....	16
<i>Low v. LinkedIn Corp.</i> , 900 F. Supp. 2d 1010 (N.D. Cal. 2012) .....	13
<i>People ex rel. Lungren v. Superior Ct.</i> , 14 Cal.4th 294 (1996) .....	21
<i>Mastel v. Miniclip SA</i> , 549 F. Supp. 3d 1129 (E.D. Cal. 2021).....	14
<i>Maya v. Centex Corp.</i> , 658 F.3d 1060 (9th Cir. 2011) .....	5
<i>Metzger v. Wells Fargo Bank, N.A.</i> , 2014 WL 1689278 (C.D. Cal. Apr. 28, 2014) .....	24
<i>Meyer v. Cap. All. Grp.</i> , 2017 WL 5138316 (S.D. Cal. Nov. 6, 2017) .....	15
<i>Multiven, Inc. v. Cisco Sys., Inc.</i> , 725 F. Supp. 2d 887 (N.D. Cal. 2010) .....	19
<i>NovelPoster v. Javitch Canfield Grp.</i> , 140 F. Supp. 3d 938 (N.D. Cal. 2014) .....	19

<i>People v. Bustamante</i> , 57 Cal. App. 4th 693 (1997) .....	13
<i>People v. Drennan</i> , 84 Cal. App. 4th 1349 (2000) .....	21
<i>Planned Parenthood v. Newman</i> , 51 F.4th 1125 (9th Cir. 2022) .....	7
<i>Pratt v. Higgins, et al.</i> , 2023 WL 4564551 (N.D. Cal. July 17, 2023).....	18
<i>Rodriguez v. Google</i> , 2021 WL 2026726 (N.D. Cal. May 21, 2021) .....	<i>passim</i>
<i>Rogers v. Ulrich</i> , 52 Cal. App. 3d 894 (1975) .....	9
<i>Rutherford Holdings, LLC v. Plaza Del Rey</i> , 223 Cal. App. 4th 221 (2014) .....	25
<i>Saroya v. Univ. of the Pac.</i> , 503 F. Supp. 3d 986 (N.D. Cal. 2020) .....	25
<i>Smith v. Facebook, Inc.</i> , 262 F. Supp. 3d 943 (N.D. Cal. May 9, 2017), <i>aff'd</i> , 745 F. App'x 8 (9th Cir. 2018).....	22
<i>Sonner v. Premier Nutrition Corp.</i> , 917 F.3d 834 (9th Cir. 2020) .....	25
<i>Stanley v. Univ. S. Cal.</i> , 178 F.3d 1069 (9th Cir. 1999) .....	24
<i>United States v. Olson</i> , 856 F.3d 1216 (9th Cir. 2017) .....	20
<i>Vess v. Ciba-Geigy Corp. USA</i> , 317 F.3d 1097 (9th Cir. 2003) .....	6
<i>Warden v. Kahn</i> , 99 Cal. App. 3d 805 (1979) .....	9
<i>Weiner v. ARS Nat'l. Servs., Inc.</i> , 887 F. Supp. 2d 1029 (S.D. Cal. 2012).....	11
<i>Wesch v. Yodlee, Inc.</i> , 2021 WL 6206644 (N.D. Cal. July 19, 2021).....	14, 18
<i>WhatsApp Inc. v. NSA Grp. Technologies Ltd.</i> , 472 F. Supp. 3d 649 (N.D. Cal. 2020) .....	16, 17

<i>White v. FIA Card Servs., N.A.</i> , 2013 WL 756292 (S.D. Cal. Feb. 26, 2013) .....	11
<i>Williams v. What If Holdings, LLC</i> , 2022 WL 17869275 (N.D. Cal. Dec. 22, 2022) .....	9, 10
<i>Yale v. Clicktale, Inc.</i> , No. 20-cv-07575-LB, 2021 WL 1428400 (N.D. Cal. Apr. 15, 2021) .....	10
<i>Zenith Ins. Co. v. O'Connor</i> , 148 Cal. App. 4th 998 (2007) .....	24

## Statutes

18 U.S.C. § 2511(2)(d) .....	7
Cal. Civ. Code § 1621 .....	24
Cal. Civ. Code § 1641 .....	22, 23
Cal. Civ. Code §§ 2924.5 and 2923.6(c) .....	24
Cal. Penal Code § 502(e)(1) .....	17, 18
Cal. Penal Code § 502(e)(2) .....	18
Cal. Penal Code § 631 .....	9, 10
Cal. Penal Code § 632(c) .....	11
Cal. Bus. & Prof. Code § 17200 .....	1, 5, 6, 13, 14
CDAFA .....	<i>passim</i>
CFAA .....	19
Electronic Communications Privacy Act, 18 U.S.C. § 2510, <i>et seq.</i> .....	5
Federal Wiretap Act, 18 U.S.C. § 2511 .....	5, 7, 8
HIPAA .....	1, 3, 4, 22
Privacy Act .....	5

## Other Authorities

Cal. Const. art. I, § 1 .....	5
California Constitution .....	12, 13
Fed. R. Civ. P. 12(b)(6) .....	1, 5

Rule 8 .....6, 8

Rule 9(b) .....6, 8, 14

## MEMORANDUM OF POINTS AND AUTHORITIES

### I. INTRODUCTION

Just as in their original Complaint, Plaintiffs’ Amended Complaint offers a tangled mess of meandering, inconsistent, and sometimes nonsensical allegations against Google. Rather than refine their allegations, Plaintiffs continue to obscure that it is developers who place the relevant cookies on Plaintiffs’ devices, not Google, and try to improperly shore up their pleadings with misconstrued evidence.<sup>1</sup> The amendments do nothing to cure the deficiencies in the original Complaint. Fundamentally, Plaintiffs still fail to explain how Google is acting as more than a mere vendor to the 12 websites at issue. This District has repeatedly recognized that developers have the right to employ analytics tools and the U.S. Department of Health & Human Services (“HHS”) itself acknowledges that healthcare website developers may use analytics tools in compliance with HIPAA. FAC Ex. 37. After all, analytics providers only provide developers with information about how users use the developers’ own properties—information the companies could analyze in-house, but choose instead to analyze using a third-party service.

Eight of the 12 claims Plaintiffs allege suffer from at least one of two fatal defects, each of which compels dismissal. *First*, Google cannot be liable for merely serving as a vendor of analytics tools to the Websites. Plaintiffs do not allege that Google directed the Websites to transmit any sensitive health data to Google in particular, or that Google did anything with *their* data other than analyze it for the Websites pursuant to the Google Analytics Terms of Service (“TOS”). While Plaintiffs make bare allegations regarding Google’s use of data for advertising, they do not allege that any data *about them* was used by Google or that they received any targeted ads following their use of the websites in question. *Second*, Plaintiffs have failed to allege that Google had the requisite knowledge or intent. The UCL, CDAFA, trespass, and conversion claims also fail because Plaintiffs lack standing and/or do not plausibly allege the requisite loss or damage. The remaining four claims also suffer from claim-specific deficiencies outlined below.

---

<sup>1</sup> For example, Plaintiffs misquote and misconstrue snippets of evidence from other cases against Google, including a proposed sur-reply in support of plaintiffs’ opposition to Google’s motion for summary judgment in *Calhoun*. See FAC ¶¶ 200-01, 340 n. 150. The Court should reject Plaintiffs’ improper attempt to salvage their pleadings in this manner.

## II. BACKGROUND

### A. Plaintiffs Allege Only That Google Lawfully Provided the Websites With Analytics Services and Other Products to Help Their Companies.

Website and app developers use a variety of products to analyze users' experiences on their properties and to market their companies, including Google products like GA, Google Tag Manager ("GTM"), Google Ads, and Google Display Network ("Display").

GA is one of the many products available in the market that allows developers to better understand how their users interact with their websites and apps. FAC. ¶ 45. It is a tool for developers to understand, among other things, their website traffic and their most popular web pages visited by users. *Id.*<sup>2</sup> Developers who implement GA choose which data is collected and how it is used. *See e.g. id.* ¶¶ 96, 121, 485 & Exs. 2, 19. Developers also choose whether and which data to share with Google, subject to contractual limitations preventing developers from sending personally identifiable information ("PII").<sup>3</sup> Unless developers enable the "data sharing with Google" setting, Google processes the data only as required to provide and maintain the GA service.<sup>4</sup> Developers may analyze patterns in user engagement using pseudonymous identifiers (strings of characters that allow developers to distinguish between users and devices), which are collected with certain events. Because the default identifiers are all pseudonymous, they are not personally identifiable. Unless both the signed-in Google account holder and developer affirmatively enable specific settings, identifiers are also limited to the visitor's session on the particular developer's property. *Id.* ¶¶ 181–83. GA then provides a report to the customer based on metrics that the customer chooses. *Id.* ¶ 118.

Google tags are lines of code used for analysis and marketing that developers may incorporate into their websites. *Id.* ¶ 96 & Exs. 2, 12. GTM is a tag management system that allows developers to deploy GA tags on their properties. *Id.* Ex. 12 at 2. Google Ads is a service companies may use to assist

<sup>2</sup> FAC ¶ 45 and Ex. 2 (*Analytics, Google Marketing Platform*, <https://marketingplatform.google.com/about/analytics/>). ("Google Analytics give you the tools, free of charge, to ... [u]nderstand how your customers interact across your sites and apps" and "analyze your data").

<sup>3</sup> RJN Ex. 4, *Data sharing settings*, <https://support.google.com/analytics/answer/1011397?hl=en#zippy=%2Cin-this-article>

<sup>4</sup> *Id.*

in marketing. *Id.* ¶ 72. Display is a fourth, separate product that has no relevance to Plaintiffs’ allegations. Developers use Display to sell advertising space on their websites to advertisers. *Id.* Ex. 26.

Plaintiffs name 12 healthcare provider web domains and one health insurance web domain that allegedly use GA: Gundersen Health System, Kaiser Permanente, Rush University System for Health, Tallahassee Memorial HealthCare, MedStar Health, Mercy Medical Center in Baltimore, MD, Mercy Hospital, OSF HealthCare, Alton Memorial Hospital – BJC Healthcare, Planned Parenthood, Shannon Medical Center, Edward-Elmhurst Health, and United Healthcare (together, the “Websites”).

**B. The Contract Between Google and the Websites Forbade the Websites From Sending Google PII, Sensitive Information About a User, or Using PII or Sensitive Information to Advertise.**

The crux of Plaintiffs’ allegations is that the relationship between the Websites and Google enabled the Websites to disclose sensitive user data to Google. But, while quoting extensively the contracts between Google and Plaintiffs for *Plaintiffs’* use of Google’s services, the FAC fails to mention the judicially noticeable foundational contracts that govern the relationships between Google and the *Websites*, which forbid the Websites from sending Google PII. Plaintiffs also ignore the privacy policies those Websites used to disclose their obligations under those contracts to users.

To use GA, developers must consent and abide by the GA TOS.<sup>5</sup> These TOS require developers to, among other things, (1) disclose their use of GA including “how it collects and processes data;” (2) disclose their use of cookies; (3) obtain user consent as required by law; and (4) refrain from sending GA any data that contains PII. *Id.* (“You will not . . . pass information . . . to Google that Google could use or recognize as [PII].”). The Google Analytics help pages for developers similarly instruct developers to, among other things, “remove PII from user-entered information before it is sent to Analytics” and ensure website URLs and titles are free from PII. FAC ¶¶ 333–34 and Ex. 54.<sup>6</sup> Further, Google prohibits developers from using GA in a way that would violate HIPAA or create any

<sup>5</sup> FAC ¶ 331 n.143 (citing *Google Analytics Terms of Service*, <https://marketingplatform.google.com/about/analytics/terms/us/>) (See RJN Ex. 1.)

<sup>6</sup> See also Ex. 55 (“Google ads product policies mandate that publishers must not pass any data to Google that Google could use or recognize as personally identifiable information (PII). This article addresses some best practices in various aspects of page design to reduce risk that PII might be in the URL that you pass to Google.”).

responsibilities *for Google* under HIPAA. FAC Ex. 1. To comply with Google’s policies, the Websites each disclose to their users the use of cookies to collect information and their use of third-party tools. RJN Exs. 6–21.

Developers who have both GA and Google Ads accounts may choose to link their accounts and use *certain* of their GA data with their Google Ads. *Id.* ¶¶ 163–65, 171. Google prohibits all developers from targeting personalized advertising based on sensitive information or prohibited categories, including personal health conditions, medication, and related health information. *Id.* Ex. 47 at 2 (“[s]ensitive interest categories are restricted in personalized ads.”). Google defines sensitive interest categories to include “health conditions, treatments, procedures, personal failings, struggles, or traumatic personal experiences,” and “personal health content,” which includes (i) “physical or mental health conditions, including diseases, sexual health, and chronic health conditions”; (ii) “products, services, or procedures to treat or manage chronic health conditions, which includes over-the-counter medications and medical devices”; and (iii) “any health issues associated with intimate body parts or functions, which includes genital, bowel, or urinary health.” *Id.* at 8.

### **C. Plaintiffs’ Allegations**

Plaintiffs are residents of Wisconsin, California, Illinois, Florida, Maryland, Nevada, and Texas who allege that they used the Websites, that those Websites transmitted Plaintiffs’ and other users’ sensitive health information to Google without Plaintiffs’ consent, and that Google profited from that information through marketing, ad targeting, and product improvement. *Id.* ¶¶ 1–7, 20–31. While Plaintiffs allege that Google matches their sensitive health information to their Google Accounts and uses this information to serve targeted ads, they do not allege that they saw any Google-served targeted advertising based on the purported health data—or any other type of data at all. *Id.* ¶¶ 106–114, 123–146.

Try as Plaintiffs might to obscure the role of the Websites through the extensive use of passive voice, the FAC nonetheless illustrates that it is the Websites that incorporate Google Source Code and control the circumstances of collection. *See id.* ¶¶ 96, 121, 485 & Exs. 2, 19.

#### **D. Procedural History**

Plaintiffs Jane Doe, et al., brought an action against Google in *Jane Doe, et al. v. Google LLC*, 5:23-cv-02343 (N.D. Cal.) on May 12, 2023. Five days later, Plaintiffs John Doe I, et al., commenced this litigation, *John Doe I, et al. v. Google LLC*, 5:23-cv-02431 (N.D. Cal.). The Court consolidated the cases on June 30, 2023. On July 13, 2023, Plaintiffs filed a motion for a preliminary injunction. Dkt. 42. Google opposed the motion and filed a motion to dismiss the Consolidated Amended Complaint. Dkt. 48. On October 18, 2023, the Court denied Plaintiffs' motion for a preliminary injunction. Dkt. 76. Plaintiffs filed their First Amended Consolidated Class Action Complaint on November 16, 2023. Dkt. 86. Plaintiffs assert the following claims against Google: Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq.* ("ECPA" or the "Wiretap Act") (Count 1); Violation of the California Invasion of Privacy Act, Cal. Penal Code. § 630, *et seq.* ("CIPA") (Count 2); Invasion of Privacy, Cal. Const. art. I, § 1 (Count 3); Intrusion Upon Seclusion (Count 4); Violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 ("UCL") (Count 5); Trespass to Chattels (Count 6); California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502 ("CDAFA") (Count 7); Breach of Express Contract (Count 8); Breach of Implied Contract (Count 9); Good Faith and Fair Dealing (Count 10); Unjust Enrichment (Count 11); and Conversion (Count 12).

#### **III. LEGAL STANDARD**

Rule 12(b)(6) requires dismissal of a cause of action that fails to state a claim upon which relief can be granted. A plaintiff must plead factual allegations that "plausibly (not merely conceivably) entitle plaintiff to relief." *Maya v. Centex Corp.*, 658 F.3d 1060, 1067–68 (9th Cir. 2011). A claim is plausible only "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (requires more than a "sheer possibility," "naked assertion" or "formulaic recitation" of the elements of a cause of action). Nor must a court "accept as true allegations that contradict matters properly subject to judicial notice or by exhibit." *Gonzalez v. Planned Parenthood of Los Angeles*, 759 F.3d 1112, 1115 (9th Cir. 2014) (citations omitted).

#### IV. ARGUMENT

Eight of the 12 claims Plaintiffs allege fail for at least one of two independent reasons: (1) Google cannot be liable for merely serving as a vendor of analytics tools to the Websites; and (2) Plaintiffs have failed to plausibly allege that Google had the requisite knowledge or intent. In addition, Plaintiffs lack standing and do not plausibly allege the requisite loss or damage for a UCL, CDAFA, trespass, or conversion claim. The remaining claims for breach of express and implied contract, breach of the implied covenant of good faith, and unjust enrichment also fail because there is no contract—express or implied—that applies to Plaintiffs’ use of third-party services, and unjust enrichment is not a cognizable claim. Several of the claims fail for additional, independent reasons, as outlined below.

##### A. The heightened standard of Rule 9(b) applies

Plaintiffs fail to meet Rule 8’s requirement of a “short and plain statement of the claim showing that the pleader is entitled to relief,” let alone the heightened specificity Rule 9(b) requires here. Rule 9(b) requires plaintiffs to plead the circumstances constituting fraud with particularity. It applies wherever a plaintiff asserts fraudulent conduct, whether or not the plaintiffs’ claim is styled as fraud. *See Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1124 (9th Cir. 2009); *Apumac, LLC v. Flint Hills Int’l*, 2015 WL 13306128, at \*5 (C.D. Cal. Feb. 6, 2015) (noting that “Rule 9(b) applies to allegations of fraud, not just claims of fraud”); *see also Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1103 (9th Cir. 2003).

Rule 9(b) applies here because Plaintiffs allege that Google collected their information by “disguising” its “secretly embedded” Source Code as first-party cookies. FAC ¶¶ 5, 57, 60(c), 290. Plaintiffs allege this collection occurs even though Google promises to the world that it will not do it. *See, e.g., id.* ¶ 289. Plaintiffs further allege that even as it makes certain promises to users, Google conspires with advertisers to break these promises. *Id.* ¶¶ 290–302. This sounds in fraud, rendering Plaintiffs’ claims subject to Rule 9(b). *See Rodriguez v. Google*, 2021 WL 2026726, at \*6 (N.D. Cal. May 21, 2021) (where plaintiffs alleged a “sensational” plot about how GA works, Rule 9(b) demanded dismissal because plaintiffs failed to allege “when the ‘secret scripts’ plot was hatched, which Google departments (let alone employees) were involved, and anything resembling a particular date, time, or place”); *Hidden Empire Holding, LLC v. Angelone*, 2023 WL 4208067, at \*17 (C.D. Cal. May 10, 2023) (noting claims involving promises without intention to honor the promise sounded in fraud).

## **B. Plaintiffs Fail to State Wiretap Claim (Count 1)**

Plaintiffs’ claim under the Federal Wiretap Act, 18 U.S.C. § 2511 is facially unsustainable and should be dismissed with prejudice for two independent reasons.

### **1. The Websites’ Consent Defeats the Wiretap Claim**

Plaintiffs’ Wiretap claim fails because one party consent is a complete defense, and the Websites consented to the use of Google Analytics. 18 U.S.C. § 2511(2)(d); Dkt. 76 at 3; *Rodriguez*, 2021 WL 2026726, at \*6. As the Websites chose to use GA, they obviously consented to it. *See* FAC ¶¶ 96, 120–121, 485 and Ex. 2 at 1 (“Tags are segments of code provided by analytics, marketing, and support vendors to help you integrate their products into your websites or mobile apps.”). This Court observed the same when rejecting Plaintiffs’ motion for a preliminary injunction. *Doe v. Google LLC*, No. 23-cv-02431-VC, 2023 WL 6882766, at \*2 (N.D. Cal. Oct. 18, 2023) (finding the website owners had consented to the use of Google Analytics on their web properties).

Plaintiffs try mightily to suggest Google does not obtain adequate consent from the Health Care Providers (as defined in the FAC ¶1 n.1) because Google can allegedly do things with the data that are contrary to its agreements with those Providers. FAC ¶¶ 307–40. Plaintiffs’ lengthy hypothetical about potential downstream uses fails because, under the plain text of the statute, the relevant consent is the permission to intercept. 18 U.S.C. § 2511(2)(d) (interception is not unlawful where a party to the communication has given consent “to such interception”). Plaintiffs have already conceded that it is the developers who determine what, if any, data to collect and transmit to Google Analytics. FAC ¶¶ 96, 121, 485 & Exs. 2, 19. They cannot now contradict those allegations in an amended pleading. *IV Sols., Inc. v. Empire Healthchoice Assurance, Inc.*, 2021 WL 5492974, at \*1 (9th Cir. Nov. 23, 2021) (“amendments to a complaint must be ‘consistent with the challenged pleading’ and must not ‘contradict[] any of the allegations of [the] original complaint.’”).

Plaintiffs offer only the barest assertion that consent is invalid because it was acquired for a “criminal” or “tortious” purpose, “including but not limited to violation of the laws set forth [in the FAC].” FAC ¶¶ 244 n.91, 338, 408, 410. Even had Plaintiffs alleged supporting facts, the “violations” set forth in the FAC stem from the same alleged interception, which is insufficient. *See Planned Parenthood v. Newman*, 51 F.4th 1125, 1136 (9th Cir. 2022) (“This criminal or tortious purpose must be

separate and independent from the act of the recording.”); *see also* Dkt. 76 at 3. Indeed, Google’s policies, which explicitly prohibit developers from sending Google any PII or PHI, demonstrate an utter lack of criminal purpose. In any event, Plaintiffs’ theory that Google “encourages” the “interception” in order to profit from it is legally deficient. *Rodriguez*, 2021 WL 2026726 at \*6 n.8 (holding Google’s “purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money”); *Katz-Lacabe v. Oracle Am., Inc.*, 2023 WL 2838118, at \*10 (N.D. Cal. Apr. 6, 2023).

## 2. Google’s Lack of Intent is Fatal to the Wiretap Claim

Plaintiffs do not plausibly allege that Google *intentionally* intercepted any communication. 18 U.S.C. § 2511. *See e.g.* FAC ¶¶ 204–224 (alleging that “Google’s conduct is knowing and intentional” because Google knows it is collecting Health Information as “Google can readily identify the web properties which use the Google Source Code” and “can easily ... identify the web properties that are Health Care Providers.”). Plaintiffs cannot plausibly allege such intent in the face of Google’s policies disclosing the *opposite* intention—that Google does not want personally identifiable information and expressly prohibits a developer from transmitting data that identifies users. *See* FAC ¶¶ 303–304, 516(e); RJN Ex.1 (“You will not and will not assist or permit any third party to pass information, hashed or otherwise, to Google that Google could use or recognize as personally identifiable information.”).

Plaintiffs’ complaint insinuates that, because Google generally offers marketing and advertising services, Google must have wanted Plaintiffs’ purported health data from the Websites so that it could “obtain significant profits from the Health Information collected.” *See* FAC. ¶¶ 224. That’s not enough to satisfy Rule 9(b), just as it wasn’t in *Rodriguez*. There is no allegation as to “when the ‘secret []’ plot was hatched; which Google departments (let alone employees) were involved; and anything resembling a particular date, time, or place.” *Rodriguez*, 2021 WL 2026726, at \*6. This theory cannot survive.

Moreover, Plaintiffs’ theory of liability is that Google surreptitiously tracks, collects, and monetizes sensitive health information. *See* FAC. ¶¶ 375, 389 (“Google’s principal goal is and was to surreptitiously monitor Plaintiffs and Class Members and to allow third parties to do the same.”). Plaintiffs come nowhere close to even meeting the Rule 8 standard, much less Rule 9(b). The judicially

noticeable documents actually disclose the opposite: that Google *required* disclosure of the use of Google Analytics and the Websites did so. RJN Ex. 1. This claim should therefore be dismissed.

### **C. Plaintiffs fail to state CIPA claims (Count 2)**

Plaintiffs' CIPA claims fail for two independent reasons: (1) Google is merely a vendor and did not "intercept" or "record" any communications, (2) Google's alleged conduct is not intentional, and (3) the Websites disclosed their use of GA.

#### **1. Google Is a Mere Vendor of an Analytics Tool to Record the Websites' Own Interactions With Users**

##### **a. CIPA Section 631**

A claim under Penal Code section 631 requires showing that Google: (1) by means of any machine, instrument, or contrivance; (2) intentionally and without the consent of all parties; (3) read, attempted to read, or to learn the contents or meaning of any communication; (4) while the communication is in transit; (5) from or to any place within California. *See Adler v. Community.com, Inc.*, 2021 WL 4805435, at \*3 (C.D. Cal. Aug. 2, 2021).

A vendor who provides a tool for a website to record user interactions is not "intercepting" a communication and cannot be liable for the recording. *Graham v. Noom*, 533 F. Supp. 3d 823, 833 (N.D. Cal. 2021); *Williams v. What If Holdings, LLC*, 2022 WL 17869275, at \*3 (N.D. Cal. Dec. 22, 2022). A party to a communication cannot violate section 631 by intercepting a communication because a party cannot wiretap itself. *See Warden v. Kahn*, 99 Cal. App. 3d 805, 811 (1979); *see also Rogers v. Ulrich*, 52 Cal. App. 3d 894, 899 (1975) (the use of a tape recorder by a party to the communication did not violate section 631). Similarly, a third-party vendor cannot violate section 631 when the vendor merely "provides a software service that captures its clients' data, hosts it on the [vendor's] servers, and allows the clients to analyze their data." *Noom*, 533 F. Supp. 3d at 832-833. In such circumstances, the third-party vendor, as a service provider, is considered to be "an extension of" the client rather than a third-party eavesdropper. *Id.* *See also Byars v. Hot Topic, Inc.*, 656 F. Supp. 3d 1051, 1068 (C.D. Cal. 2023) (holding that the allegation that the defendant allowed "at least one third party to eavesdrop on such communications in real time and during transmission to harvest data for financial gain" was conclusory, and that "stor[ing] transcripts of Defendant's chat communications with 'unsuspecting'

website visitors” does not make the defendant's vendor an eavesdropper); *Johnson v. Blue Nile, Inc.*, No. 20-cv-08183-LB, 2021 WL 1312771 (N.D. Cal. Apr. 8, 2021) at \*1 (third-party vendor which used “session replay” software to record website activities of defendant's visitors was an extension of defendant); *Yale v. Clicktale, Inc.*, No. 20-cv-07575-LB, 2021 WL 1428400, at \*1, \*3 (N.D. Cal. Apr. 15, 2021) (same, with “Event-Triggered Recorder” software). Thus, a service provider to a party stands in the shoes of that party—or as an extension thereof—and similarly cannot violate section 631.

*Noom* is directly on point. There, defendant Noom used the defendant FullStory’s software to record “visitor data such as keystrokes, mouse clicks, and page scrolling,” which allegedly resulted in the disclosure of “medical information” to FullStory without consent. *Noom*, 533 F. Supp. 3d at 823–29. The court held this could not violate CIPA because FullStory acted as a service provider to Noom, and the plaintiff did not plausibly allege that FullStory “aggregate[ed] [the] data for resale . . . [or that it] used the data itself.” *Id.* Accordingly, at most, the defendant provided a “tool” that allowed Noom to “record and analyze its own data in aid of Noom’s business.” *Id.* In light of these circumstances, the court held that FullStory “is an extension of Noom,” as opposed to a third-party eavesdropper. *Id.* at 832-33.

Judge Alsup’s reasoning in *Williams* also applies here: as alleged, Google is a third-party vendor that was hired as a service provider to process records of the Websites’ communications with their end users, and Google’s software was merely a tool that the Websites used to record aspects of those communications with plaintiffs. *Williams*, 2022 WL 17869275, at \*3 (“[R]ecordation is routine documentation and therefore clerical in nature, which is qualitatively different from data mining.”). That the vendor stores and processes the data on its own servers “is part of how the software tool functions” and does not by itself subject the vendor to liability. *Id.* As in *Noom*, Google provides a software service to the Websites and thereby functions as “an extension of” the Websites, rather than as a third-party eavesdropper.

The bare and conclusory allegations that Google “is not a mere vendor” and that Google’s activity “amounts to data mining” does not assist Plaintiffs. FAC ¶¶ 115-122. It is plain on the face of the Complaint that it is developers who choose what content they wish to send Google, including

whether anything constituting a “communication” is transmitted, and whether to share their data with Google such that Google may use it to improve its products. *See, e.g.*, FAC ¶¶ 40, 96–97, 108–110, 126, 140–142 & Exs. 14–15. The Websites authorized Google—as their vendor—to receive the communications at issue and therefore Google could not have “intercepted” the alleged “communications” as a matter of law. Plaintiffs do not allege that Google instructed the Websites to transmit to Google the purported health data—or any other type of data at all. And, contrary to Plaintiffs’ bare and false allegations, Google does not share GA data with third parties. *See* FAC ¶¶ 4, 98–100, 116.<sup>7</sup> Plaintiffs’ Wiretap claim should therefore be dismissed.

### **b. CIPA Section 632**

Plaintiffs’ section 632 claim fails for similar reasons. To state a claim under section 632, a plaintiff must allege that the defendant (1) “intentionally and without [] consent,” (2) recorded a “confidential communication,” (3) by means of an electronic device. *See* Cal. Penal Code § 632; *Weiner v. ARS Nat’l. Servs., Inc.*, 887 F. Supp. 2d 1029, 1032 (S.D. Cal. 2012).

Here, Plaintiffs cannot allege that Google “recorded” a “confidential communication” for two reasons. First, the alleged recording was performed by the Websites, not Google. *See* FAC ¶¶ 96, 121, 485 & Exs. 2, 19. Second, section 632 does not apply where “the parties to the communication may reasonably expect that the communication may be overheard or recorded.” Cal. Penal Code § 632(c). Because each of Plaintiffs’ Health Care Providers disclosed their data collection and use, Plaintiffs had no reasonable expectation of privacy in their analytics data on the Websites. RJN Exs. 6–21; *White v. FIA Card Servs., N.A.*, 2013 WL 756292, at \*5 (S.D. Cal. Feb. 26, 2013) (no reasonable expectation of privacy where agreement notified consumers that calls may be monitored). Plaintiffs’ claim under section 632 must therefore fail.

### **2. Google’s lack of intention is fatal to CIPA claims**

Plaintiffs’ CIPA claims also fail because Plaintiffs do not plausibly allege that Google intentionally intercepted their PHI. *See supra* section IV.B(2). The policies and restrictions Google

---

<sup>7</sup> Plaintiffs’ only factual allegation in support of this assertion, namely that GTM shares GA or Ads data with any third-party entity whose code a developer has also chosen to incorporate into its property through GTM, lacks common sense and is unsupported by the help pages they cite.

implements, and the fact that the Health Care Providers control what they send to Google, undermine the naked assertions that Google intended to intercept Plaintiffs' PHI. *See* FAC ¶¶ 303–304, 516(e).

**D. Privacy Claims Should be Dismissed (Counts 3 and 4)<sup>8</sup>**

California's common law intrusion-upon-seclusion claim requires a plaintiff to plead that (1) "the defendant [] intentionally intrude[d] into a place, conversation, or matter, as to which the plaintiff has a reasonable expectation of privacy," and (2) "the intrusion [] occur[ed] in a manner highly offensive to a reasonable person." *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286 (2009). The common law "set[s] a high bar for an invasion of privacy claim." *Belluomini v. Citigroup, Inc.*, 2013 WL 3855589, at \*6 (N.D. Cal. July 24, 2013).

Plaintiffs plead insufficient facts to state a plausible claim for invasion of privacy because (1) Google did not have the requisite intent; and (2) there can be no highly invasive intrusion where Google is not an unauthorized third party.

**First**, setting aside Plaintiffs' bare assertions of intent (*see* FAC ¶ 443), their allegations regarding Google's policies against the at issue collection, and the fact that developers control what data is transmitted, negate their claims that Google "intended" to violate their privacy. *See Caraccioli v. Facebook, Inc.*, 167 F. Supp. 3d 1056, 1063 (N.D. Cal. 2016), *aff'd*, 700 F. App'x 588 (9th Cir. 2017) ("intrusion upon seclusion . . . require[s] intent on the part of the tortfeasor" and plaintiff failed to plead Facebook's intent where "the allegations in the amended complaint contradict the incorporated Terms of Service").

**Second**, Plaintiffs' invasion of privacy claims are premised on Google's alleged "unauthorized access" to the purported communications. *See* FAC ¶ 437 ("Plaintiffs' and Class Members' claims are based on Google's unauthorized access to their Health Information."). Because Google was an authorized vendor to the Websites, Google could not have engaged in an unauthorized intrusion at all—much less one that is highly offensive to a reasonable person. *See, e.g., Noom*, 533 F. Supp. 3d at 835–36 ("Because there was no plausible wiretapping by [vendor defendant], the plaintiffs did not plausibly

---

<sup>8</sup> The elements for invasion of privacy under the California Constitution (Claim 3) and for the common law claim of intrusion upon seclusion (Claim 4) are sufficiently similar that courts consider them together. *In re Facebook*, 956 F.3d at 601. The analysis here thus applies equally to both claims.

plead that they possess a legally protected privacy interest.”); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1024–25 (N.D. Cal. 2012) (“The California Constitution and the common law set a high bar for an invasion of privacy claim. Even the disclosure of personal information . . . does not constitute an ‘egregious breach of the social norms’ to establish an invasion of privacy claim”) (collecting cases); *see also In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 830 (N.D. Cal. 2020) (dismissing intrusion upon seclusion claim where Plaintiffs failed to state Federal Wiretap claim and CIPA claim). Plaintiffs fail to state a common law or constitutional privacy claim.<sup>9</sup>

#### **E. Plaintiffs’ UCL Claim Should be Dismissed (Count 5)**

Plaintiffs’ UCL claim fails because Plaintiffs (1) lack UCL standing and (2) fail to plausibly plead knowledge.

*First*, “the UCL limits standing to those who have ‘suffered injury in fact and lost money or property as a result of . . . unfair competition.’” *Rodriguez*, 2021 WL 2026726, at \*8 (citation omitted). “[C]ourts have widely held that ‘personal information’ does not constitute money or property under the UCL.” *Gardiner v. Walmart, Inc.*, 2021 WL 2520103, at \*8 (N.D. Cal. Mar. 5, 2021); *Oracle*, 2023 WL 2838118, at \*8 (dismissing UCL claim for lack of standing because “the ‘mere misappropriation of personal information’ does not establish compensable damages”); *Rodriguez*, 2021 WL 2026726, at \*8 (“[N]o federal court has wedged individual digital data into the UCL’s ‘money or property’ box”); *Gonzalez v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1093 (N.D. Cal. 2018), *on reconsideration*, 2018 WL 3068248 (N.D. Cal. June 21, 2018) (“[T]he sharing of names, user IDs, location and other personal information does not constitute lost money or property for UCL standing purposes.”). Plaintiffs’ allegations that Google may benefit from their data does not cure the deficiency. FAC. ¶¶ 341–368; *see, e.g., Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1040 (N.D. Cal. 2019) (“That the information has external value, but no economic value to plaintiff, cannot serve to establish that plaintiff has personally lost money or property.”).

---

<sup>9</sup> In addition, the California Constitution does not apply extraterritorially and cannot be applied to out-of-state Plaintiffs. *See People ex rel. DuFauchard v. U.S. Fin. Mgmt., Inc.*, 169 Cal. App. 4th 1502, 1516 (2009) (statutes are presumed not to apply extraterritorially); *People v. Bustamante*, 57 Cal. App. 4th 693, 699 n.5 (1997) (constitutional provisions and statutes construed the same way).

Nor do Plaintiffs allege that they suffered economic injury independent of Google’s “secret” data collection, such as expenditures in reliance on any misrepresentations Google made. In any event, for Plaintiffs’ harm to be “fairly traceable” to Google’s alleged misrepresentations under the UCL, “Plaintiffs must have seen the misrepresentations and taken some action based on what they saw.” *In re iPhone Application Litig.*, 6 F. Supp. 3d 1004, 1015 (N.D. Cal. 2013) (finding no UCL standing where Plaintiffs failed to establish actual reliance on Apple’s alleged misrepresentations). Here, Plaintiffs do not allege that they read *any* other Google representation, in connection with their use of the Websites or otherwise. FAC. ¶ 468; see *Rodriguez*, 2021 WL 2026726, at \*8 (no UCL standing where plaintiffs did not contend that any transactions were taken “because of [their] understanding of the [App’s] data practices vis-a-vis Google.”).<sup>10</sup>

**Second**, under the “unfair” (and “fraudulent”) prongs of the UCL, Plaintiffs allege, in conclusory fashion, that “Google assures users of all Google products that it will not collect Health Information without users’ consent but in reality *knows* (or should have known) that the Google Source Code and advertising products are being improperly used on Health Care Provider web properties.” FAC. ¶ 463 (emphasis added). Because the basis of Plaintiffs’ claims under these prongs sound in fraud, Plaintiffs must plead them with particularity. *See, e.g., Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009) (a UCL claim that is “grounded in fraud” “must satisfy the particularity requirement of Rule 9(b)”). They have not come close to doing so. In fact, Google’s policies disclose the *opposite* intention—that Google does not want personally identifiable information and expressly prohibits a developer from transmitting data that identifies users. *See* FAC ¶¶ 303–304, 516(e); RJN Ex.1. *See also supra* section IV.B(2).

---

<sup>10</sup> The court in *Calhoun* held that allegations of the loss of personal information sufficiently stated an “economic injury” under the UCL. *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 636 (N.D. Cal. 2021). But courts have subsequently rejected this holding as erroneous. As explained by another judge in this District, *Calhoun* relied on cases addressing Article III standing, which is distinct. *See, e.g., Cottle v. Plaid Inc.*, 536 F. Supp. 3d 461, 484 n.8 (N.D. Cal. 2021) (“This court disagrees with the holding in *Calhoun*.”). And as another judge in this District explained, the UCL case *Calhoun* cited for its holding rejected the conclusion that *Calhoun* reached. *Wesch v. Yodlee, Inc.*, 2021 WL 6206644, at \*4 (N.D. Cal. July 19, 2021) (“Additionally, *Calhoun* cites *In re Facebook Privacy Litigation* as support for standing under the UCL, but the Ninth Circuit explicitly rejected this theory in that case.”); *see also Mastel v. Miniclip SA*, 549 F. Supp. 3d 1129, 1145 (E.D. Cal. 2021).

## **F. Claims for Trespass to Chattels and Conversion Fail (Counts 6 and 12)**

“Trespass to chattels lies where an intentional interference with the possession of personal property has caused injury.” *Best Carpet Values, Inc. v. Google LLC*, 2021 WL 4355337, at \*4 (N.D. Cal. Sept. 24, 2021) (citing *Intel Corp. v. Hamidi*, 30 Cal. 4th 1348, 1350–51 (2003)). Where, as here, the trespass concerns “unauthorized electronic contact with computer systems,” the plaintiff must establish that the contact damaged the computer system or impaired its functioning. *Intel*, 30 Cal. 4th at 1352.

“To establish conversion, a plaintiff must show ‘ownership or right to possession of property, wrongful disposition of the property right and damages.’” *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1074 (N.D. Cal. 2012) (citing *Kremen v. Cohen*, 337 F.3d 1024, 1029 (9th Cir.2003)).

“Conversion requires a higher showing than trespass, which has been dubbed the “little brother of conversion.” *Meyer v. Cap. All. Grp.*, 2017 WL 5138316, at \*9 (S.D. Cal. Nov. 6, 2017) (citing *Intel*, 30 Cal. 4th at 1350). It follows that if Plaintiffs fail to allege facts sufficient to support trespass, they also fail to allege facts to support conversion. *Id.* Aside from conclusory assertions, Plaintiffs fail to allege facts sufficient to support any element of these claims.

### **1. Failure to Allege Intent**

Claims for trespass and conversion require the defendant’s *intentional* interference with the plaintiff’s personal property. *Best Carpet*, 2021 WL 4355337, at \*4 (trespass); *Doe v. Roblox Corp.*, 602 F. Supp. 3d 1243, 1264 (N.D. Cal. 2022) (conversion requires “that the defendant disposed of the plaintiff’s property rights or converted the property by a wrongful act.”) (quotations omitted). Although Plaintiffs offer the bare assertion that Google intentionally placed cookies on Plaintiffs’ devices, Plaintiffs’ factual allegations establish the opposite. Indeed, Plaintiffs illustrate that it is the Websites that “deployed the Google Source Code” and “had Google Cookies lodged on [the Plaintiffs’] computing device[s].” FAC ¶ 485; *see also id.* ¶ 40 (“Google Source Code is provided by Google in a copy-and-paste format.”).

### **2. No Interference with Plaintiffs’ Personal Property**

The torts of trespass and conversion protect *possessory* interests in property. *Intel*, 30 Cal. 4th at 1359 (trespass); *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1074 (conversion). Plaintiffs’

argument that their “personal information” is capable of exclusive possession has previously been rejected by California courts. *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1075 (“[T]he weight of authority holds that a plaintiff’s ‘personal information’ does not constitute property.”); *Alderson v. United States*, 718 F. Supp. 2d 1186, 1197 (C.D. Cal. 2010) (“In order to possess a property right, whether tangible or intangible, a person must be able to exclude others from using or taking the purported property.”). In fact, Plaintiffs’ complaint focuses on data that was never in Plaintiffs’ possession. *See, e.g.*, FAC ¶ 25 (alleging, albeit wrongly, that the data is solely in Google’s possession and Plaintiffs are unaware of what data may have been collected from them). Plaintiffs allege that the data at issue concerns Plaintiffs’ activities on third-party websites. *See, e.g.*, FAC ¶¶ 36, 53–65, 592. This information would not exist but for the intervention of the software the Websites deployed for their own purposes. Since the Health Care Providers create the data and control whether and to what extent others may access it, it is the Health Care Providers, not the Plaintiffs, that could have any possessory interest in the data, assuming California law recognizes such an interest in the first instance.

Indeed, California courts have held that allegedly unauthorized copying of electronic information, without more, fails to implicate a cognizable property interest. *See Casillas v. Berkshire Hathaway Homestate Ins.*, 79 Cal. App. 5th 755, 764–65 (2022) (rejecting trespass claim based on copying of files and collecting authorities); *Intel*, 30 Cal. 4th at 1361–62 (“[T]he appropriate tort is not trespass.”).

### **3. Plaintiffs Fail to Plausibly Allege Actual Loss**

Plaintiffs do not and cannot plausibly allege damage to or loss of function of their devices. *Intel*, 30 Cal. 4th at 1147. California courts routinely hold that the placement of cookies or the interception or copying of personal data is insufficient to support the “actual loss” requirement of a trespass claim—some damage to the computer or loss of function. *See, e.g., Casillas*, 79 Cal. App. 5th at 764; *WhatsApp Inc. v. NSA Grp. Technologies Ltd.*, 472 F. Supp. 3d 649, 685–86 (N.D. Cal. 2020) (dismissing trespass claim based on the installation of malware on plaintiff’s servers that diverted communications to defendants); *LaCourt v. Specific Media, Inc.*, 2011 WL 1661532, at \*7 (C.D. Cal. Apr. 28, 2011) (defendant’s alleged placement of tracking cookies for targeted advertisement did not result in the impairment required to state a claim for trespass); *In re iPhone Application Litig.*, 844 F. Supp. 2d at

1069 (allegation that defendant’s apps took up bandwidth and storage on plaintiffs’ devices “do not plausibly establish a significant reduction in service constituting an interference with the intended functioning of the system.”). And, Plaintiffs do not even attempt to allege that the alleged damage to their devices constitutes conversion. *See* FAC ¶¶ 591–98.

Plaintiffs offer the naked assertion that the alleged trespass caused the “total deprivation of Plaintiffs’ and Class Members’ use of their computing devices to communicate with Health Care Providers,” (FAC ¶ 495(f)), but this unsupported assertion makes no sense and was correctly rejected in a parallel case brought by Plaintiffs’ counsel against a Health Care Provider. In *Kurowski*, the court found that the plaintiffs could not plausibly allege that the placement of cookies degrades the functionality of the plaintiffs’ devices where, as here, the plaintiffs had alleged that the Health Care Provider’s “placement of cookies was so invisible and surreptitious that she was completely unaware of it.” *Kurowski v. Rush Sys. for Health*, No. 22 C 5380, 2023 WL 4707184, at \*10 (N.D. Ill. July 24, 2023). Further, common sense dictates that Google cannot “intercept” any communications if Plaintiffs are unable to use their devices for communicating with providers. Far from rendering the devices inoperable, the allegations at the center of Plaintiffs claims rely on their devices functioning as intended. *See WhatsApp*, 472 F. Supp. 3d at 659–60 (dismissing trespass claim based on the installation of malware where the allegations demonstrated the malware relied on the plaintiff’s servers functioning as intended). Consistent with California law, the Court should reject Plaintiffs’ nonsensical effort to manufacture a trespass claim.

### **G. Plaintiffs Fail to State a CDAFA Claim (Count 7)**

Plaintiffs have no statutory standing to bring an action under CDAFA because they fail to allege any damage or loss. Cal. Penal Code § 502(e)(1). Additionally, Plaintiffs do not plausibly allege that Google knew it lacked authorization for the complained-of conduct.

#### **1. Standing under CDAFA**

CDAFA permits a civil action only by a person “who suffers damage or loss by reason of a violation.” Cal. Penal Code § 502(e)(1). Plaintiffs claim they suffered “damages and losses” including: (1) the inability of Plaintiffs to communicate with Health Care Providers; (2) a sense of violation and loss of trust in Plaintiffs’ Health Care Providers; (3) resources expended to investigate and respond to

Google’s alleged violations; (4) diminution of value of Plaintiffs’ Health Information; and (5) diminution of storage space on and speed of Plaintiffs’ computers. FAC ¶¶ 518. None of these alleged “losses” support Plaintiffs’ claim.

First, Plaintiffs’ allegations contradict the assertion that Google disrupted Plaintiffs’ ability to communicate with Health Care Providers. By Plaintiffs’ own account, the alleged data acquisition can only occur when Plaintiffs communicate with the providers, and Plaintiffs allege they were unaware of the cookies. FAC ¶¶ 491, 516(c); *Kurowski*, 2023 WL 4707184, at \*10.

Second, there is no authority that Plaintiffs’ subjective feelings about their Health Care Providers constitutes a cognizable loss. *See Pratt v. Higgins, et al.*, 2023 WL 4564551, at \*9 (N.D. Cal. July 17, 2023) (dismissing claim that accessing medical information gave rise to any cognizable loss under CDAFA).

Third, Plaintiffs’ vague allegation that they expended resources to “investigate” the alleged violations is insufficient. Under the statute’s plain terms, compensable investigation costs are limited to those “reasonably and necessarily incurred . . . to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access.” Cal. Penal Code § 502(e)(1). Whatever Plaintiffs may have done to “investigate” purported violations, Plaintiffs make no allegation that they investigated whether Google “altered, damaged, or deleted” their data, or that they incurred costs in the course of such an investigation.<sup>11</sup> Nor could Plaintiffs plausibly suggest they “reasonably and necessarily” incurred investigative costs to discover cookies and practices that both their Health Care Providers and Google directly disclosed.

Fourth, courts have rejected Plaintiffs’ “diminution of value” theory, particularly where, as here, the plaintiffs do not demonstrate that they were ready and willing to market their personal data. *See, e.g., Cottle*, 536 F. Supp. 3d at 484; *Wesch*, 2021 WL 6206644, at \*5; *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 149 (3d Cir. 2015).

---

<sup>11</sup> The only “investigation” Plaintiffs allege is the “the investigation of counsel.” FAC ¶ 518(a). Holding that such legal costs are “damages and loss” within the meaning of section 502(e)(1) would render the legislature’s separate allowance for attorneys’ fees superfluous. Cal. Penal Code § 502(e)(2). If one could evade the “damage or loss” limitation simply by retaining counsel, there would be no lawsuit in which the “damage or loss” limitation has any effect.

Finally, Plaintiffs’ allegations that Google occupied storage space and resources on Plaintiffs’ computers and caused the computers to work slower are conclusory and fall short of a plausible claim. Not one of the Plaintiffs alleges that he or she discerned any difference in the performance of his or her computer while visiting the Websites. Quite the opposite, Plaintiffs allege that they had no knowledge of Google’s alleged cookie placement, and when it suits them—seeking to toll the statute of limitations—Plaintiffs claim the tracking was “undetectable by patients” and could not be discovered even through reasonable diligence. FAC ¶¶ 389, 486, 595. *See Kurowski*, 2023 WL 4704184, at \*10 (concluding that plaintiff did not plausibly allege any injury or interference with her devices where she alleged she was completely unaware of the placement of cookies). Courts have found such allegations insufficient to state a claim under the federal analog to CDAFA, the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030.<sup>12</sup> *See In re iPhone Application Litig.*, 844 F. Supp. 2d at 1066–67 (citing *Del Vecchio v. Amazon.com, Inc.*, 2011 WL 6325910, at \*4 (W.D.Wa. Dec. 1, 2011) (concluding that Plaintiffs failed to establish damages under the CFAA where Plaintiffs had not alleged that they “discerned any difference whatsoever in the performance of [their] computer while visiting Defendants’ site”); *Bose v. Interclick, Inc.*, 2011 WL 4343517, at \*4, 2011 U.S. Dist. LEXIS 93663, at \*12–14 (S.D.N.Y. Aug. 17, 2011) (finding that Plaintiff’s allegation that Defendant “impaired the functioning and diminished the value of Bose’s computer” was general and failed to quantify the alleged repair cost); *Czech v. Wall St. on Demand, Inc.*, 674 F.Supp.2d 1102, 1118 (D. Minn. 2009) (holding that a plaintiff’s claim that unwanted text messages “caused the wireless devices of [Plaintiff] to slow and/or lag in operation” and “impair[ ] the availability of and interrupt[ ] the wireless-device service” was conclusory and insufficient for a CFAA claim)). Plaintiffs thus cannot establish standing under CDAFA.

## 2. Plaintiffs Cannot Establish Google Knew Its Collection was Unauthorized

While Plaintiffs assert that Google’s alleged collection was unauthorized (see FAC ¶ 516), they fail to establish Google knew it acted without permission. “Absent indication of contrary purpose in the

---

<sup>12</sup> Courts apply the definitions of “damage” and “loss” found in CFAA to CDAFA. *See, e.g., NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 951 (N.D. Cal. 2014) (pleading was deficient in alleging damage or loss under CDAFA “for the same reason” as CFAA claim was defective); *Multiven, Inc. v. Cisco Sys., Inc.*, 725 F. Supp. 2d 887, 895 (N.D. Cal. 2010) (“the necessary elements of [CDAFA] do not differ materially from the necessary elements of the CFAA for purposes of “damages or loss ....”).

language or legislative history of the statutes, [courts] ordinarily read a phrase in a criminal statute that introduces the elements of a crime with the word ‘knowingly’ as applying that word to each element.” *United States v. Olson*, 856 F.3d 1216, 1220 (9th Cir. 2017). Here, the elements of CDAFA, a criminal statute, are introduced with the word ‘knowingly,’ and there is no indication that the legislature intended to impose strict liability on individuals who accessed data under a good faith but mistaken belief of authorization. *See id.* Plaintiffs must not only allege that Google lacked permission, they must show Google knew it lacked permission. *See id.*

The closest Plaintiffs come is alleging that “Google’s own policies prohibit Google from accessing and using Plaintiffs’ and Class Members’ Health Information.” FAC ¶ 516(e). But that fact demonstrates that Google had all the less reason to know that Health Care Providers would send any PHI. And in any event, whether or not *Google’s* policies permit access does not bear on whether Google knew *Plaintiffs* did not authorize the alleged access. Further, while Plaintiffs assert that Google’s Search infrastructure is capable of determining which categories of websites *may* implicate PHI (*id.* ¶¶ 204–23), they also contend Google “does not use its systems or the data transmitted therein to require Health Care Providers to comply with applicable law, to respect privacy rights, or to refrain from engaging in misleading or fraudulent conduct in the unlawful tracking, collection and disclosure to Google of patients’ Health Information.” (*Id.* ¶¶ 290, 543).

In essence, Plaintiffs assert that Google has the *capability* to determine that there is a *possibility* that certain websites *might* be able to transmit PHI, but that Google does not use that capability to affirmatively identify the at-risk websites. Even then, Plaintiffs offer no explanation for how identifying the at-risk websites would put Google on notice that the websites were actually transmitting PHI—a critical omission given Plaintiffs’ admission that developers choose which data to transmit to GA.<sup>13</sup> Plaintiffs’ allegations thus refute that Google knew it acted without authorization. *See In re A.L.*, 38 Cal. App. 5th 15, 21 (2019) (holding actual knowledge means subjective awareness of necessary facts).

---

<sup>13</sup> These allegations highlight the illogical catch-22 underlying all of Plaintiffs’ scienter allegations. It is not enough that Google forbids developers from sending it PHI, according to Plaintiffs. They would impose a duty upon Google to affirmatively review the developer’s data to determine whether PHI is being transmitted. Obviously, doing so would require Google to intrude into the private data and learn its contents—creating the very intrusion Plaintiffs complain of.

## H. No Breach of Contract (Count 8)

Plaintiffs base their contract claim on Google’s TOS and Privacy Policy. Those claims fail because the TOS and Privacy Policy apply by their plain terms to Plaintiffs’ use of Google’s services, not Plaintiffs’ use of third-party services that may also use Google’s services.<sup>14</sup> Even assuming the TOS and Privacy Policy apply here, Plaintiffs blatantly alter their text in the Complaint to suit their narrative.

### 1. Alleged Breach One

Plaintiffs first allege that Google broke a promise in its TOS that Google would enforce applicable laws and its policies against third-parties. But the plain text of the TOS provided that Plaintiffs had to comply with all applicable laws. This term was a promise made by Plaintiffs, not Google. The same section makes clear that Plaintiffs’ remedy for third-party violations was simply to report the violation to Google. RJN Ex. 5 at 5 (“If you find that others aren’t following these rules, many of our services allow you to report abuse.”). It is equally clear that Google made no promise to take action on such reports. *Id.* (“***If*** we act on a report of abuse . . .”) (emphasis added). Plaintiffs’ absurd reading would require Google to be a global enforcer of all laws applicable to any Google user.

### 2. Alleged Breach Two

Plaintiffs assert a variety of other purported breaches of Google’s Privacy Policy. Plaintiffs claim Google breached a representation that Google collects health information “if you choose to provide it.” But the information Plaintiffs accuse here—pseudonymous event metadata concerning Plaintiffs’ activity on healthcare websites—is not the “health information” described in the Privacy Policy, which concerns the actual medical records or metrics about a specific person.

The *noscitur a sociis* canon provides that a word “takes meaning from the company it keeps.” *People v. Drennan*, 84 Cal. App. 4th 1349, 1355 (2000). “In accordance with this principle of construction, a court will adopt a restrictive meaning of a listed item if acceptance of a more expansive meaning would . . . make the item markedly dissimilar to the other items in the list.” *People ex rel. Lungren v. Superior Ct.*, 14 Cal.4th 294, 307 (1996). The “health information” referred to in the Privacy Policy includes “medical history, vital signs and health metrics (like blood glucose levels), and other

---

<sup>14</sup> Google’s TOS list the services that they govern. None of the services at issue here are listed. *See* <https://policies.google.com/terms/service-specific?hl=en-US>.

similar information.” RJN Ex. 3 at 18. “Health information,” therefore, means actual medical history and metrics about a person, not the URLs and event data associated with a pseudonymous identifier that may, or may not, have any relation to health. *See Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 954–55 (N.D. Cal. May 9, 2017), *aff’d*, 745 F. App’x 8 (9th Cir. 2018) (URLs for pages “containing information about treatment options for melanoma, information about a specific doctor, [or] search results related to the phrase ‘intestine transplant’” are not PHI); *Kurowski*, 2023 WL 4707184, at \*4 (browsing metadata on healthcare provider’s website “does not in the least bit fit” into the category of individually identifiable health information covered by HIPAA). This is confirmed by the separate provision for collection of web activity, search terms, and other information on third party websites. Cal. Civ. Code § 1641 (“[T]he whole of a contract is to be taken together, so as to give effect to every part, if reasonably practicable, each clause helping to interpret the others.”). Because “health information” as used in the Privacy Policy refers to actual medical information rather than web activity data from which assumptions may be made about a person, Plaintiffs’ second breach of contract theory fails.

### 3. Alleged Breach Three

Plaintiffs’ third theory of breach claims that Google breaks its promise not to personalize advertisements based on Health Information. Plaintiffs’ allegations fail to support this theory of breach, and none alleges he or she received a personalized advertisement based on PHI.

Aside from repeating the conclusory assertion that Google allows personalized advertisements based on personal health information (*see, e.g.*, FAC ¶ 123), Plaintiffs’ only factual allegations are off the mark. Plaintiffs identify Google’s policies and restrictions that allow “healthcare-related advertising” in some circumstances. *Id.* ¶¶ 291–92. But Google does not promise to prohibit healthcare-related advertisements generally. It prohibits personalized advertisements based on the users’ sensitive health data. *Id.* ¶¶ 282–83. Google’s Privacy Policy makes clear that “personalized ads” refers to advertising based on information Google collects about the user. RJN Ex. 3 at 6–7 (informing that Google uses “the information [it] collect[s]” about the user to personalize services, including ads). Because Plaintiffs’ allegations go no further than suggesting Google permits generalized, non-personalized healthcare advertising, Plaintiffs’ third theory of breach fails.

This theory fails for the additional reason that no Plaintiff alleges he or she ever received a personalized advertisement based on their PHI (or even any generalized healthcare-related ads). Plaintiffs thus cannot show that they have suffered a breach, and they lack standing to assert a claim for the mere risk that they or someone else could see an offending advertisement. *See Cahen v. Toyota Motor Corp.*, 717 F. App'x 720, 724 (9th Cir. 2017) (affirming dismissal of contract and other claims based on a risk of hacking).

#### **4. Alleged Breach Four**

Plaintiffs assert that Google does not “use its systems” to prevent the purportedly “unlawful tracking, collection and disclosure” of their information, in violation of a purported promise to protect users from illegal activity. FAC ¶¶ 290, 543. This is another manipulation of the Privacy Policy’s plain text.

Plaintiffs quote from a portion of the Privacy Policy purporting to explain what data Google collects from a user and how Google uses that user’s data. RJN Ex. 3 at 18. It is not a statement about Google’s use of its “systems” or other technologies. Similarly, the portion Plaintiffs quote does not refer to the use of users’ data to protect users, but rather the use of such data for Google’s own purposes, such as to protect Google systems. The header above the quoted language—“[b]usiness purposes for which information may be used or disclosed”—makes this clear. *Id.* This is consistent with all other provisions in the section, which focus on how Google uses data internally for its own “business purposes.” *See Cal Civ. Code* § 1641 (a provision should be construed in light of the surrounding provisions). This provision cannot be read as an open-ended promise to users for Google to use “its systems” to protect against any “security threats, abuse, [or] illegal activity” they may encounter online.

#### **I. No Breach of Implied Contract (Count 9)**

Plaintiffs seek to assert a duplicative claim for breach of an implied contract between Google and its users. Because an express contract applies to these users, an implied contract claim is unavailable. *Hammerling*, 615 F. Supp. 3d 1069, 1095–96 (N.D. Cal. 2022). Plaintiffs also purport to assert an implied contract claim on behalf of those who do not have a Google Account, which is coextensive with the claims asserted on behalf of users, but fail to support any such claim.

“An implied contract is one, the existence and terms of which are manifested by conduct.” Cal. Civ. Code § 1621. It is unclear what “conduct” Plaintiffs contend created the contract. For instance, Plaintiffs claim Google made “express promises,” but an implied contract is, by definition, one in which “the agreement and promise have not been expressed in words.” *Stanley v. Univ. S. Cal.*, 178 F.3d 1069, 1078 (9th Cir. 1999). Nor do Plaintiffs claim Google made these promises to non-users in any particular way, or that the non-users saw them, relied on them, or otherwise intended for these promises to form the basis for their agreement with Google. *See* FAC ¶ 548(a).<sup>15</sup> In these circumstances, Plaintiffs fail to establish a “*mutual agreement and intent*” necessary to support an implied contract. *Gorlach v. Sports Club Co.*, 209 Cal. App. 4th 1497, 1508 (2012) (emphasis in original).

Plaintiffs also point to their subjective expectations of privacy. *Id.* ¶ 548(c). But unilateral, subjective expectations fail to support an implied contract. *See Zenith Ins. Co. v. O’Connor*, 148 Cal. App. 4th 998, 1010 (2007).

Finally, Plaintiffs point to federal, state, and common law protections regarding Health Information. Statutes, however, are not private contracts, nor are they automatically incorporated into contracts. *See e.g., Metzger v. Wells Fargo Bank, N.A.*, 2014 WL 1689278, at \*7 (C.D. Cal. Apr. 28, 2014) (“With respect to the alleged failure by Wells Fargo to comply with Cal. Civ. Code §§ 2924.5 and 2923.6(c), an implied covenant is based on the terms of the contract, rather than statutory duties imposed.”). In any event, because Plaintiffs have not established a breach of the express contract, their duplicative implied contract claim likewise fails.

#### **J. No Breach of the Implied Covenant of Good Faith and Fair Dealing (Count 10)**

Plaintiffs allege a breach of the implied covenant of good faith by “intercepting their Health Information.” FAC ¶ 564. Because Plaintiffs allege that the express terms of their contract with Google covers the handling of their “Health Information,” (*see* FAC ¶¶ 536–37, 541–42), they cannot assert an implied covenant claim for the same conduct. *See Careau & Co. v. Sec. Pac. Bus. Credit, Inc.*, 222 Cal. App. 3d 1371, 1395 (1990) (“If the allegations do not go beyond the statement of a mere contract breach and, relying on the same alleged acts, simply seek the same damages or other relief already claimed in a

---

<sup>15</sup> Indeed, insofar as an implied contract is defined by conduct, Plaintiffs contend Google’s conduct was inconsistent with these promises. *Id.* ¶¶ 554–560.

companion contract cause of action, they may be disregarded as superfluous as no additional claim is actually stated.”). To the extent the handling of Health Information is not covered by the terms of the alleged contracts, the claim would still fail; the implied covenant cannot impose new contractual duties beyond those found in the contract. *Guz v. Bechtel Nat’l Inc.*, 24 Cal. 4th 317, 249 (2000).

**K. Unjust Enrichment Is Not Cognizable (Count 11)**

An unjust enrichment claim is not a standalone claim under California law and is construed as a quasi-contract claim. *Saroya v. Univ. of the Pac.*, 503 F. Supp. 3d 986, 998 (N.D. Cal. 2020). Such a claim is inappropriate where Plaintiffs allege that a valid, express contract covers the same subject matter. *Id.*; *Rutherford Holdings, LLC v. Plaza Del Rey*, 223 Cal. App. 4th 221, 231 (2014). Plaintiffs cannot maintain both contract and unjust enrichment actions “unless the plaintiff also pleads facts suggesting that the contract may be unenforceable or invalid,” which Plaintiffs fail to do here. *Saroya*, 503 F. Supp. 3d at 998.

Further, despite the conclusory assertion that Plaintiffs lack an adequate remedy at law, they allege a host of legal claims seeking the same relief—the value of their data. *See, e.g.*, FAC ¶¶ 559(d)–(e); 567(e); see also *Sonner v. Premier Nutrition Corp.*, 917 F.3d 834, 844 (9th Cir. 2020) (affirming dismissal of unjust enrichment claim where plaintiff sought the same relief in equitable restitution as in damages). Plaintiffs unjust enrichment claim should be dismissed.

**V. CONCLUSION**

For the foregoing reasons, Google respectfully requests that the Court dismiss the FAC.

Dated: December 21, 2023

**WILLKIE FARR & GALLAGHER LLP**

By: /s/ Benedict Hur  
 Benedict Hur  
 Simona Agnolucci  
 Eduardo Santacana  
 David Doak  
 Joshua Anderson  
 Tiffany Lin  
 Harris Mateen  
 Naiara Toker

Attorneys for Defendant  
 GOOGLE LLC